Product Certification System

Umbrella Document for

eIDAS (Electronic Identification and Signatures)

KPMG Certification Body FLCES 006

Enforcement steps:	**Name:**	**Date:**
Created by scheme owner	Philipp Wirth	08.06.2022
Controlled by proxy scheme owner	Reto Grubenmann	15.07.2022
Released by	Reto Grubenmann	15.07.2022
Review of scheme operation		

Vaduz, 15.07.2022

1 Table of Content

2 Introduction

2.1 Description

The eIDAS Regulation introduces mutual recognition of electronic IDs and electronic trust services, including electronic signatures. An electronic signature can be defined as data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign.

KPMG certification body FLCES 006 aims to assess the client's conformity with the requirements which are set forth in the various certification schemes listed in the product overview. Based on the scope of application, the client can assess their organizational framework and technical infrastructure according to five product certification schemes related to the eIDAS regulation: Qualified Electronic Signatures (A), Qualified Electronic Seals (B), Qualified Electronic Timestamps (C), Qualified Preservation of Qualified Electronic Signatures (D), and Remote Identity Verification (E).

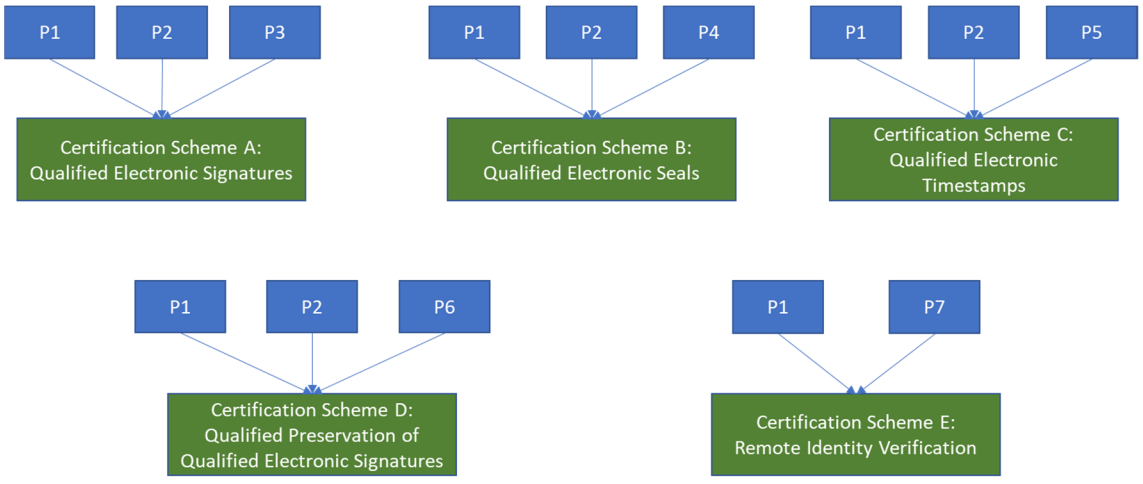
KPMG certification body FLCES 006 is accredited based on DIN ES ISO/IEC 17065 in conjunction with the ISO/IEC 17067 and regulation (EU) 910/2014 including ETSI EN 319 403.

2.2 Product Overview

The KPMG Certification Body FLCES 006 maintains five different product certification schemes related to the eIDAS regulation:

- *Product Certification Scheme A: Qualified Electronic Signatures*
- *Product Certification Scheme B: Qualified Electronic Seals*
- *Product Certification Scheme C: Qualified Electronic Timestamps*
- *Product Certification Scheme D: Qualified Preservation of Qualified Electronic Signatures*
- *Product Certification Scheme E: Remote Identity Verification*

The five certification products are modularly designed, as shown in the figure below:



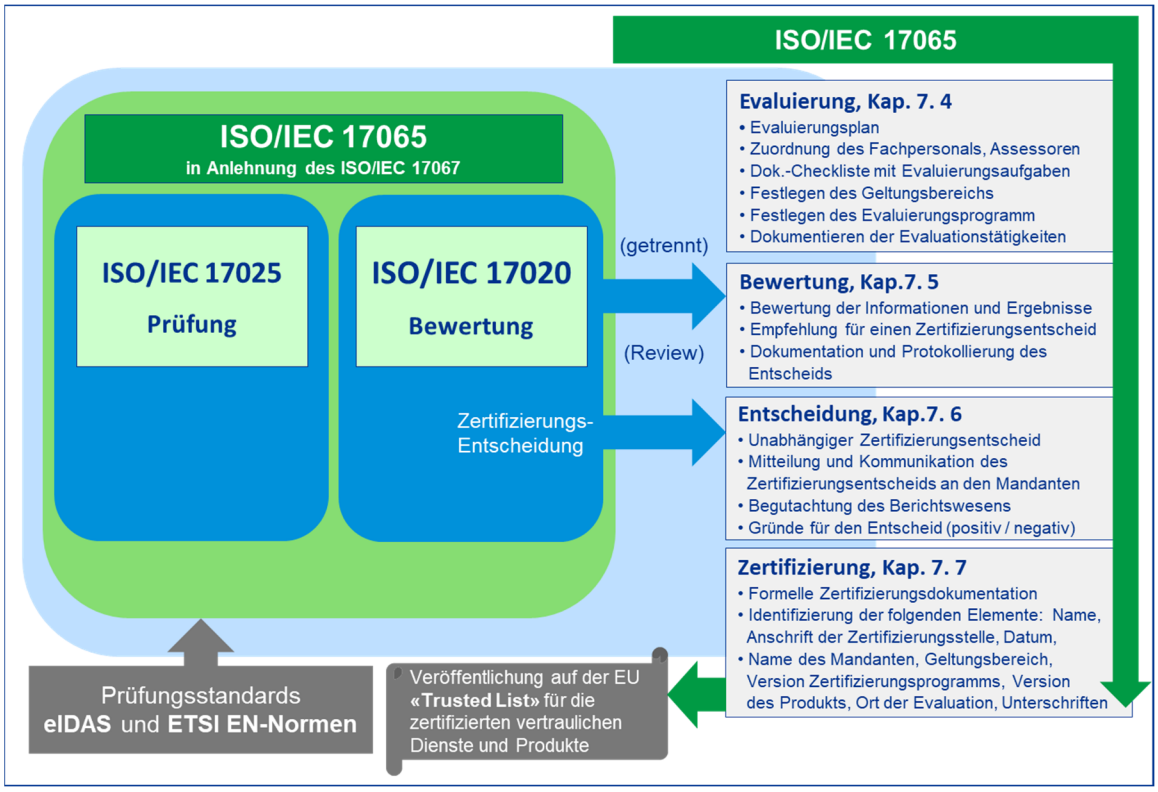
The modules P1 to P7 correspond to requirements from different norms and standards as follows:

Module	Norm / Standard	Description	Version
P1	ETSI EN 319 401	Electronic Signatures and Infrastructure (ESI); General Policy Requirements for Trust Service Providers	V2.3.1 (2021-05)
P2	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements	V1.3.1 (2021-05)
	ETSI EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates	V2.4.1 (2021-11)
	ETSI TS 119 312	Cryptographic suites for secure electronic signatures	V1.4.2 (2022-02)
	IETF RFC 5280	X.509 Internet Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	2018-05
	IETF RFC 3647	X.509 Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework	2003-11
	IETF RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	2013-06
P3	ETSI EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures	V1.4.4 (2021-05)
	ETSI EN 319 412-2	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons	V2.2.1 (2020-07)
	ETSI EN 319 412-5	Certificate Profiles; Part 5: QCStatements	V2.3.1 (2020-04)
	DIN EN 419 241-1	Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements	2018-09
P4	ETSI EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures	V1.4.4 (2021-05)
	ETSI EN 319 412-3	Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons	V1.2.1 (2020-07)
	ETSI EN 319 412-5	Certificate Profiles; Part 5: QCStatements	V2.3.1 (2020-04)
P5	ETSI EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps	V1.1.1 (2016-03)
	ETSI EN 319 422	Time-stamping protocol and time-stamp token profiles	V1.1.1 (2016-03)

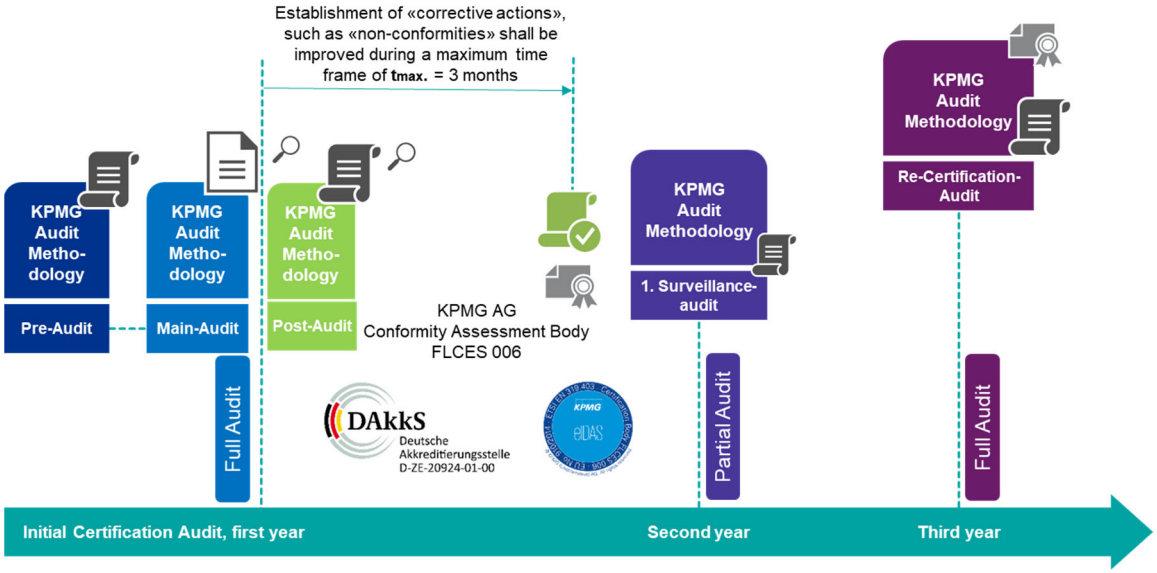
P6	ETSI TS 119 511	Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques	V1.1.1 (2019-06)
	ETSI TS 119 512	Protocols for trust service providers providing long-term data preservation services	V1.1.2 (2020-10)
P7	ETSI TS 119 461	Policy and security requirements for trust service components providing identity proofing of trust service subjects	V1.1.1 (2021-07)

3 Audit Methodology

The following picture shows the different audit activities for the eIDAS certification:



The certification body will assess the certification scheme based on the following audit frequency:



4 Allocation of Audit Programs and Procedures

The following table shows the activities and the output that the client can expect at the end of each phase:

Phase / Activities	Output
Selection: Scoping / Meeting	Scope Template with scope of scheme including the type of product covered
Application for Certification	Application Template
Certification Contract (2 years contract)	- Certification Contract - Audit Methodology - Commercials - General Terms of Business (GTB)
Audit Plan	Audit Plan with Dates and Time, Interviewer, Location and Set of controls
Opening Meeting	Presentation
Planning / Interviews / Walkthroughs / Technical Console Testing	- List of control objectives according to Audit plan - Document Checklist

Phase / Activities	Output
Evaluation: - Documentation Audit (Stage I) - Implementation Audit (Stage II) - Technology and Process Analysis and Synthesis (Findings, Observations and Recommendations)	- Results of review - Stage I&II Audit report (Documentation Review and Evaluation)
Review: Appraisal of Testing Results: - Evaluation of test results with regards of fulfillment of the required standards - Verification of adequacy of performed determination activities.	n/a
Decision	Decision on certification with validation of conformity and non-conformity (time-imposed control objectives)
Closing Meeting	Meeting with information about corrective actions (minor non-conformities, major non-conformities)
Reporting for Certification	Audit report
Post-Audit (Verification of Improvements)	- Final report with remarks to improved non-conformities (date) - Time imposed non-conformities (if applicable)
Certification: Conformation for official Certification	- Issuance of Certification - Registration of Certification Number - Norm and Standards
Surveillance: Surveillance Audit	- Planning Meeting, Audit Plan - Stage I, Stage II Audit - Audit Reporting
Recertification	- Application - Evaluation - Review - Decision - Audit Reporting - Issuance of Certification

5 Product certification requirements

The descriptions of the schemes (1a – 6) are described in appendix A (Type of product certification schemes).

No.	Assessment functions and activities	1a	1b	2	3	4	5	6
I	**Selection**, including planning and preparation activities, specification of requirements, e.g. normative documents, and sampling:							
	a) Documentation checklist provided by KPMG							X
	b) Scope template							X
II	**Determination of characteristics:**							
	a) Testing of design (control description)							X
	b) Inspection, walkthrough							X
	c) Design appraisal (concept of TSP trust services)							X
	d) Assessment of services or processes (certificates, infra-structure, security management, certificate management, registration)							X
	e) Validation of evidences							X
	f) Interviews and verification of controls							X
	g) Testing or inspection of samples within the premises of TSP							X
	h) Testing of technical profile of signatures							X
	i) Assessment of the operation of the process.							X
III	**Review/ Initial Certification Audit:** Examining the evidence of conformity obtained during the determination stage to establish whether the specified re-quirements have been met:							
	a) Stage I Audit (Documentation Review)							X
	b) Stage II Audit (Implementation Review)							X
	c) Post Audit (Verification of corrective actions)							X
IV	**Decision on certification:** Granting, maintaining, extending, reducing, suspending, withdrawing certification:							
	a) Registration of Certification (trusted list)							X
	b) Issuance of official Certification							X
	c) Issuance of Service Seals/ Symbols							X
V	**Attestation, licensing:**							
	a) Issuing a certificate of conformity or other statement of conformity (attestation).							X
	b) Granting the right to use certificates or other statements of conformity.							X
	c) Issuing a certificate of conformity for service.							X

No.	Assessment functions and activities	1a	1b	2	3	4	5	6
	d) Granting the right to use marks of conformity is based on surveillance or certification of a batch.							
VI	**Surveillance Audit by:** a) Testing or inspection of TSP (trusted service provider).							X
	b) Testing or inspection of samples within the premises of TSP.							X
	c) Testing of technical profile of signatures							X
	d) Assessment of the operation of the process.							X
	e) Management system audits combined with random tests or inspections.							X

6 Formal Application of Clients

Potential customers should deliver following information to KPMG in case of a formal application for an eIDAS certification:

Doc. #	Document name	Description incl. expected content
01	Scope eIDAS template	To define the scope for the certification with all processes and technical assets.
02	Certification Policy (CP)	A Certification Policy (CP) is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. In general, there are two major categories of CPs: - Focused on indication applicability of a certificate to a particular community (e.g. geographical region, specific market – finance, assurance etc.); - Focused on indication applicability of a certificate to class of application with common security requirements (e.g. different level of security and level of assurance).
03	Certification Practice Statement (CPS)	Certification Practice Statement (CPS) is the document supporting the Certification Policies, describing the operating part of public key certification process, participants of this process (Certification Authorities, Registration Authorities, Subscribers and Relying Parties) and describing the areas of application of certificates obtained as its result. CPS should answer for question “how”.
04	Inventory of assets	A detailed inventory of hardware and software is necessary for recovery and integrity purposes.

Doc. #	Document name	Description incl. expected content
05	Service description	Description of the service that is offered and is planned to certify.

7 Responsibilities

Following parties are involved in this product certification with different responsibilities:

- KPMG (Liechtenstein) AG (FLCES 006): Conformity Assessment Body (CAB)
- Deutsche Akkreditierungsstelle GmbH (DAkkS): Accreditation Body
- Amt für Kommunikation (AK) Liechtenstein: Administration of „Trusted List“
- BundesNetzAgentur (BNetzA) Bonn: Member of accreditation commission
- Bundesamt für Sicherheit in der Informationstechnik (BSI)

Appendix A: Content of Scheme

Elements of product certification scheme	Definition of KPMG's CAB
a) scope of the scheme;	a) scope eIDAS (EU) Reg. 910/2014, ETSI EN 319.403
b) requirements against reference to standards or other normative documents;	b) See chapter 4 in this document
c) Activities	c) see chapter 6 in this document
d) Other requirements to be met by the client;	d)No additional requirements that have to be meet by the client (for requirements see chapter 4 in this document)
e) requirements for certification bodies and other conformity assessment bodies involved in the certification process;	e) KPMG's CAB will fulfill all requirements
f) conformity assessment bodies are accredited on the same level as KPMG CAB;	f) If activities will be outsourced to third parties, KPMG will ensure that the third parties fulfill the requirement of the relevant standards
g) the methods and procedures to be used by the conformity assessment bodies	g) see chapter 3 and 6 in this document
h) the information need for applicant for certification;	h) According to scope template
i) the content of the statement of conformity (e.g. certificate)	i) See certificate templates for eIDAS certfication
j) conditions for use of the statement of conformity or marks of conformity;	j) the use of conformity or marks of conformity will be governed by the rules of the KPMG certification body and its QM-handbook
k) requirements regarding the management of marks of conformity	k) see j)
l) the resources required for the operation of the scheme,	l) KPMG has two subject matter expert in this expert area
m) how the results of the determination (evaluation) and surveillance stages are to be reported and used	m) the reporting and usage of the results is according to ISO/IEC 17065, Section 7.7.1

Elements of product certification scheme	Definition of KPMG's CAB
n) the question of how non-conformities with the certification requirements, which include product requirements, are to be dealt with and resolved;	n) the handling of non-conformities is according to ISO/IEC 17065, Section 7.6
o) surveillance procedures, where surveillance is part of the scheme;	o) the surveillance procedures are according to ISO/IEC 17065, Section 7.9
p) the criteria for access of conformity assessment bodies to the scheme and for the access of clients to the scheme;	p) KPMG does not allow third parties to access the product conformity assessment scheme.
q) content, conditions and responsibility for publication of the directory of certified products by the certification body or the scheme owner;	q) the publication of the directory of certified products is according to ISO/IEC 17065, Section 7.8
r) the need for, and content of, contracts	r) the need for contracts is according to ISO/IEC 17065, Section 7.2
s) general conditions for granting, maintaining, continuing, extending the scope of, reducing the scope of, suspending and withdrawing certification:	s) The general conditions for granting, maintaining, continuing, extending the scope of, reducing the scope of, suspending and withdrawing certification are following the process of the KPMG CAB.
t) the way in which the clients' complaints records are to be verified if such verification is part of the scheme;	t) KPMG will assess the procedures client complaints and the risk impact of the received complains. This verification will be performed due the requirements of the applicable EN-Norms.
u) Using the scheme in publicity material;	u) All references to certification and scheme are governed under the agreement between KPMG and the client
v) retention of records by scheme owner and certification bodies.	v) the retention of records is according to ISO/IEC 17065, Section 7.12

Appendix B: Type of product certification schemes

Type 1a: In this **scheme, one or more samples of the product are subjected to the determination activities.** A certificate of conformity or other statement of conformity is issued for the product type, the characteristics of which are detailed in the certificate or a document referred to in the certificate. Subsequent production items are not covered by the certification body's attestation of conformity. The samples are representative of subsequent production items which could be referred to by the manufacturer as being manufactured in accordance with the certified type. The certification body may grant to the manufacturer the right to use the type certificate or other statement of conformity (e.g. letter) as a basis for the manufacturer to declare that subsequent production items conform to the specified requirements.

Type 1b: This scheme type involves the certification of a whole batch of products, following selection and determination as specified in the scheme. The proportion to be tested, which can include testing of all the units in the batch (100% testing), would be based, for example, on the homogeneity of the items in the batch and the application of a sampling plan, where appropriate. If the outcome of the determination, review and decision is positive, all items in the batch may be described as certified and may have a mark of conformity affixed, if that is included in the scheme.

Type 2: The surveillance part of this scheme involves periodically taking samples of the product from the market and subjecting them to determination activities to check that items produced subsequent to the initial attestation fulfil the specified requirements.

While this scheme may identify the impact of the distribution channel on conformity, the resources it requires can be extensive. Also, when significant nonconformities are found, effective corrective measures may be limited since the product has already been distributed to the market.

Type 3: The surveillance part of this scheme involves periodically taking samples of the product from the point of production and subjecting them to determination activities to check that items produced subsequent to the initial attestation fulfil the specified requirements. The surveillance includes periodic assessment of the production process.

This scheme does not provide any indication of the impact the distribution channel plays on conformity. When serious nonconformities are found, the opportunity may exist to resolve them before widespread market distribution occurs.

Type 4: The surveillance part of this scheme allows for the choice between periodically taking samples of the product from the point of production, or from the market, or from both, and subjecting them to determination activities to check that items produced subsequent to the initial attestation fulfil the specified requirements. The surveillance includes periodic assessment of the production process.

This scheme can both indicate the impact of the distribution channel on conformity and provide a premarket mechanism to identify and resolve serious nonconformities. Significant duplication of effort may take place for those products whose conformity is not affected during the distribution process.

Type 5: The surveillance part of this scheme allows for the choice between periodically taking samples of the product either from the point of production, or from the market, or from both, and subjecting them to determination activities to check that items produced subsequent to the initial attestation fulfil the specified requirements. The surveillance includes periodic assessment of the production process, or au-

dit of the management system, or both. The extent to which the four surveillance activities are conducted may be varied for a given situation, as defined in the scheme. If the surveillance includes audit of the management system, an initial audit of the management system will be needed.

Type 6: This **scheme is mainly applicable to certification of services and processes**. Although services are considered as being generally intangible, the determination activities are not limited to the evaluation of intangible elements (e.g. effectiveness of an organization's procedures, delays and responsiveness of the management). In some situations, the tangible elements of a service can support the evidence of conformity indicated by the assessment of processes, resources and controls involved. For example, inspection of the cleanliness of vehicles for the quality of public transportation.

As far as processes are concerned, the situation is very similar. For example, the determination activities for welding processes can include testing and inspection of samples of the resultant welds, if applicable. For both services and processes, the surveillance part of this scheme should include periodic audits of the management system and periodic assessment of the service or process.